(19) Europäisches Patentamt
European Pat nt Offic
Office européen des brevets

(11) EP 0 718 803 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
26.06.1996 Bulletin 1996/26

(51) Int Cl.[6]: **G07B 17/04**

(21) Application number: **95120424.7**

(22) Date of filing: **22.12.1995**

(84) Designated Contracting States:
DE FR GB

(30) Priority: **22.12.1994 US 361409**

(71) Applicant: **PITNEY BOWES INC.**
Stamford Connecticut 06926-0700 (US)

(72) Inventors:
- **Lee, Young W.**
  Orange, Connecticut 06477 (US)
- **Moh, Sungwon**
  Wilton, Connecticut 06897 (US)
- **Muller, Arno**
  Westport, Connecticut 06880 (US)

(74) Representative: **Avery, Stephen John et al**
Hoffmann, Eitle & Partner,
Patent- und Rechtsanwälte,
Arabellastrasse 4
81925 München (DE)

(54) Identifying a specific combination of metering accounting vault and digital printer

(57) For preventing monitoring of postage indicia data which is sent from a postage metering vault to a remotely located digital printer (21) over a communication link (C11) between the meter vault and the digital printer (21). the meter (11) is provided with an encryption engine (37) for encrypting postage indicia data utilizing an encryption key. The digital printer (21) includes a decryption engine (53) for decrypting postage data received from said meter (11) utilizing the same encryption key and then prints a postage indicia pursuant to the decrypted postage indicia data. The postage meter (11) also includes a key manager (39) for generating new encryption key pursuant to a token which is either randomly generated or generated pursuant to an algorithm by a similar encryption key manager (61) located in the digital printer (21), which token is also used to generate the decryption key for the decryption engine (53). As a result, the encryption keys are the same. Upon power-up of the system or at such other preselected times, the print controller module of the digital printer (21) sends out an encrypted message to the meter (11). The message consist of a random number. The encryption/decryption engine (37) of the vault decrypts the message. The vault then returns an encrypted new message to the print controller (23) which includes an encoded representation of the relationship of the two messages. Upon receiving the new message from the vault, the print controller (23) decrypts the new message and verifies the relationship. The print controller (23) is then enabled to print a postage indicia.

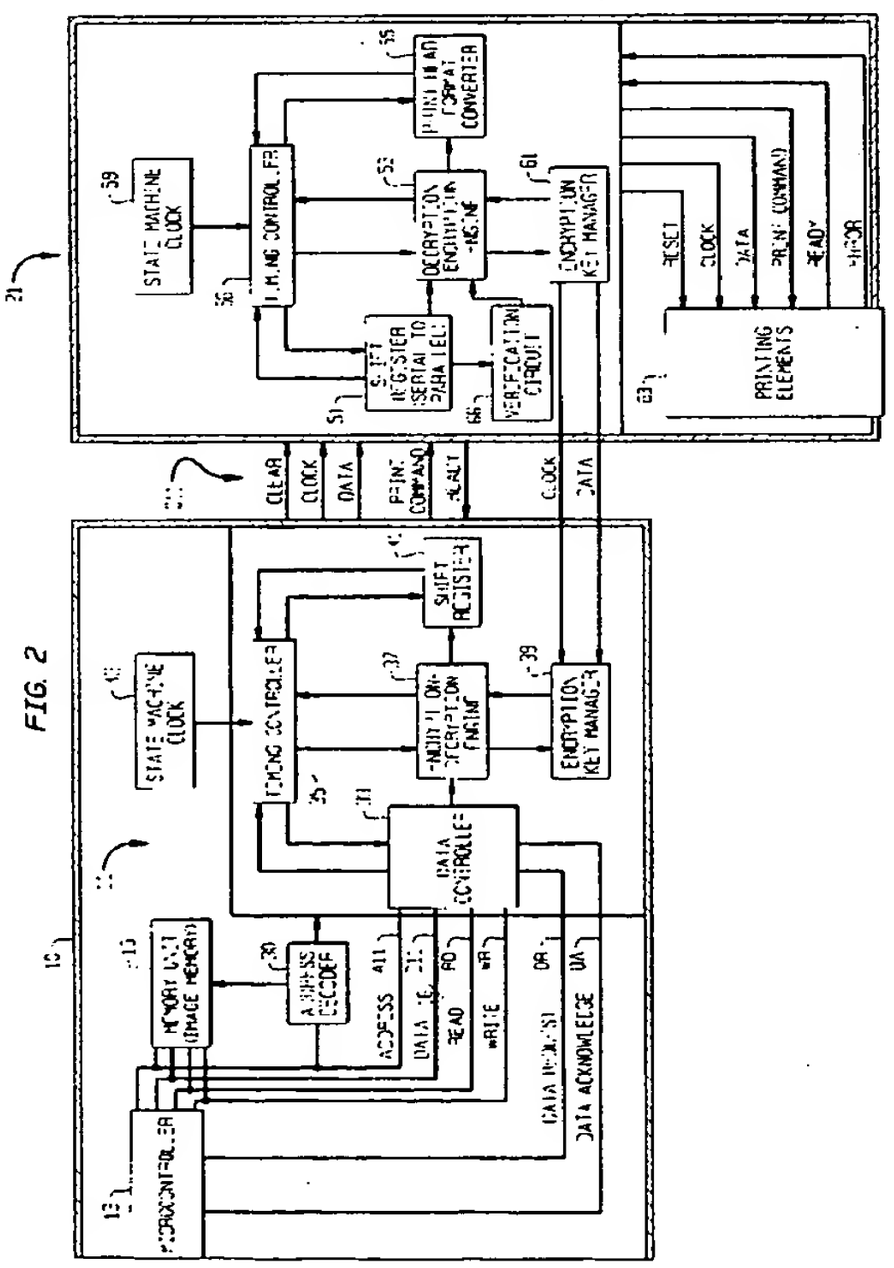

FIG. 2

EP 0 718 803 A2

Printed by Jouve, 75001 PARIS (FR)

Description

The present invention relates to a postage metering system using digital printing and, more particularly, to a postage metering system wherein the postage accounting system is remotely located from the postage printer.

A conventional postage meter is comprised of a secure account system, also known as a vault, and an impact printing mechanism housed in a secure housing having tamper detection. The vault is physical secured and operationally interlocked to the printing mechanism. For example, it is now known to use postage meters employing digital printing techniques. In such systems, the vault and digital printer remain secure within the secure housing and printing can only occur after postage has been accounted for.

It is also known to employ a postage meter in combination with an inserting system for the processing of a mail stream. It has been determined that it would be beneficial to configure a postage metering system which employs an inserter and digital printer in combination with a remotely located vault. However, it has also been determined as a security step to be beneficial to provide a means to assure that an authorized vault is driving the digital printers in order to insure proper postal accounting between the system user and postal services. Further, such systems may be equipped with remote funds resetting capability, therefore, it is necessary that the accounting records of the user, postal service and operator of the remote funds reset center be reconcilable with regards to a identifiable combination of vault and digital printing systems.

It is an object of the present invention to present a method of preventing the operation of a digital printer to print a postage indicia unless the digital printer is in electronic communication with a specific vault system.

A new metering system includes a meter in bus communication with a digital printer for enabling the meter to be located remote from the digital printer. The meter includes a vault which is comprised of a micro controller in bus communication with an application specific integrated circuit (ASIC) and a plurality of memory units secured in a tamper resistant housing. The ASIC includes a plurality of control modules, some of which are an accounting memory security module, a printer controller module and a encryption module. The digital printer includes a decoder/encoder ASIC sealed to the print head of the digital printer. The decoder/encoder ASIC communicates to the printer controller module via a printer bus. Communication between the printer controller and the print head decoder/encoder ASIC interface is accomplished through a printer bus which communications are encrypted by any suitable known technique, for example, using a data encryption standard (DES) algorithm. By encrypting the output of the printer controller module along the printer bus any unauthorized probing of the output of the printer controller to acquire and store the signals used to produce a valid postage print are prevented. If the electrical signals are probed, the data cannot easily be reconstructed into an indicia image by virtue of the encryption. The print head decoder consists of a custom integrated circuit located in proximity to the printing elements. It receives the output from the printer controller, decrypts the data, and reformats the data as necessary for application to the printing elements.

The printer controller and print head controller contain encryption key manager functional units. The encryption key manager is used to periodically change the encryption key used to send print data to the print head. The actual keys are not sent over the interface, rather, a token representing a specific key is passed. The key can be updated every time the printer controller clears the print head decoder, after a particular number of print cycles, or after a particular number of state machine clock cycles. By increasing the number of encryption keys, the probability that the system will be compromised diminishes.

In order to assure full and accurate accounting for the particular digital printer, upon power-up of the system or at such other preselected condition, the print controller module of the digital printer sends out an encrypted message to the meter. This message consists of an encrypted random number. The encryption/decryption engine of the postage meter decrypts the message. The meter then returns an encrypted new message to the print controller which includes an encoded representation of the relationship of the two messages. Upon receiving the new message from the vault, the print controller decrypts the new message and verifies the relationship. The print controller is then enabled to print a postage indicia.

Fig. 1 is a diagrammatic representation of a postage meter in combination with a remote printing mechanism in accordance with the present invention.

Fig. 2 is a diagrammatic representation of the postage meter micro control and printer micro control systems in accordance with the present invention.

Referring to Fig. 1, the postage meter control system 11 is comprised of a micro controller 13 in bus communication with a memory unit 15 and ASIC 17. The printing mechanism 21 is generally comprised of a print controller 23 which controls the operation of a plurality of print elements 27. Data is communicated between the meter control system 11 and the print mechanism over a bus C11. Generally, print data is first encrypted by an encryption module 18 and presented to the printer controller 23 through a printer controller module 19 of the ASIC 17. The data received by the print controller 23 is decrypted by a decryption module 25 in the print mechanism 21 after which the print controller 23 drives the print elements 27 in accordance with the received data. The data exchanged between the two devices is subject to interception and possible tampering since the electrical interconnects are not physically secured. Utilizing encryption to electrically secure the interface between the printer controller and print head reduces the ability

of an external intrusion of data to the print mechanism 21 to drive unaccounted for posting by the printing mechanism 21. If the electrical signals are probed, the data cannot easily be reconstructed into an indicia image by virtue of the encryption. The print head mechanism 21 consists of a custom integrated circuit ASIC, more particularly described subsequently, located in proximity to the printing elements to allow physical security such as by epoxy sealing of the ASIC to the print head substrate utilizing any suitable known process.

Referring to Fig. 2, the meter control system 11 is secured within a secure housing 10. More specifically, a micro controller 13 electrically communicates with an address bus A11, a data bus D11, a read control line RD, a write control line WR, a data request control line DR and a data acknowledge control line DA. The memory unit 15 is also in electrical communication with the bus A11 and D11, and control lines RD and WR. An address decoder module 30 electrically communicates with the address bus A11. The output from the address decoder 30 is directed to a data controller 33, timing controller 35, encryption/decryption engine 37, encryption key manager 39 and shift register 41. The output of the address controller 30 operates in a conventional manner to enable and disable the data controller 33, timing controller 35, encryption engine 37, encryption key manager 39 and shift register 41 in response to a respective address generated by the micro controller 13.

The data controller 33 electrically communicates with the address bus and data bus A11 and D11, respectively, and also with the read and write control lines RD and WR, respectively. In addition, the data controller 33 electrically communicates with the data request DR and data acknowledge DA control lines. The output from the data controller 33 is directed to an encryption/decryption engine 37 where the output data from the data controller 33 is encrypted using any one of several known encryption techniques, for example, the DES encryption algorithm. The output from the encryption engine 37 is directed to the shift register 41. The timing controller 35 electrically communicates with the data controller 33, the encryption/decryption engine 37 and shift register 41 for providing synchronize timing signals to the data controller 33, the encryption/decryption engine 37 and shift register 41. The timing controller 35 receives a input clock signal from a state machine clock 43. In the most preferred configuration, a encryption key manager 39 is in electrical communication with the encryption/decryption engine 37 for the purposes of providing added system security in a manner subsequently described.

The printer mechanism 21 control ASIC includes a shift register 51, decryption/encryption engine 53 and a print head format converter 55. The output from the shift register 51 is directed to the input of the decryption/encryption engine 53. The output of the decryption/encryption engine 53 is directed to the print head format converter 55. The timing controller 56 electrically communicates with the shift register 51, decryption/encryption engine 53, print head format converter 55 for providing synchronized timing signals to the data controller 33, the encryption/decryption engine 37 and shift register 41. The timing controller 56 receives a input clock signal from a state machine clock 59. In the most preferred configuration, a encryption key manager 61 is in electrical communication with the encryption/decryption engine 53 for the purposes of providing added system security and communicating with the encryption key manager 39 of the meter control system 11. The printer control ASIC electronically communicates with the print elements 63. Also provided is a verification circuit 66 which receives data from the shift register 41 only during system power-up and outputs data to the decryption/encryption engine 53.

In operation, upon power-up of the system or at such other selected times, the verification circuit in response to a power-up print command (Print Cmmd) from the meter control system 11 outputs a random number message to the decryption/encryption engine which encrypts the message in response to the power-up print command. The encrypted message is sent out to the meter. The encryption/decryption engine 37 of the vault decrypts the message in response to the print command. The micro controller then returns an encrypted new message to the print controller which includes the encoded representation of the relationship of the two messages. Upon receiving the new message from the vault, the print controller decrypts the new message and verifies the relationship in response to a new print command. The print controller is then enabled to print a postage indicia. The print controller is now enabled resulting in the engine 33 being set in a encryption mode and engine 53 being set in a decryption mode.

Upon initiation of a print cycle, the micro controller 13 generates the appropriate address and generates an active write signal. The less significant bits (LBS) of the generated address is directed to the address decoder 30 and the most significant bits (MBS) are directed to the data controller 33. In response, the address decoder 30 generates the enable signals for the data controller 33, timing controller 35, encryption engine 37 and shift register 41. The data controller 33 then generates a data request which then is received by the micro controller 13. The micro controller 13 then generates a read enable signal which enables the micro controller 13 to read the image data from the memory unit 15 and place the appropriate data on the data bus D11. That data is read by the data controller 33 which reformats the 32-bit data messages into 64-bit data messages and passes the 64-bit data messages to the encryption engine 37. The encryption engine 37 then encrypts the data using any suitable encryption algorithm and the encryption key supplied by the encryption key manager 39. The encrypted data is then passed to the shift register 41 for serial communication of the encrypted data to the printer 21. The operation of the data controller 33, encryption engine 37 and shift register 41 is synchronized by the

timing controller 35 which receives a clocking signal from the state machine clock 43.

Over a communication bus C11, the encrypted serial data output from the shift register 41 is directed to the shift register 51 of the printer 21. Also carried over the bus C11 are the appropriate clock signals for clocking the data into the shift register 51 and a print command (Print Cmmd). When the whole of the encrypted information has been transmitted, a clear signal is generated over the bus C11. The shift registers 51 of the printer 21 reformats the encrypted data back into 64-bit parallel form and transfers the 64-bit data messages to the decryption engine 53 which decrypts the data using the same key used to encrypt the data which is provided by the encryption key manager 61. The decrypted data is then received by the print format converter 55 for delivery to the print head driver which enables the appropriate printing elements. It should now be appreciated that the process described in particularly suitable for any form of digital printer, such as, ink jet or thermal. Once the printing process has been completed a ready signal is sent to the meter over the bus C11.

The function of the encryption key manager in both printer controller and print head controller is to periodically change the encryption key used to send print data to the print head. The actual keys are not sent over the interface, rather, a token representing a specific key is passed. This token may be the product of an algorithm which represents any desired compilation of the data passed between the meter and the printer over some predetermined period. The token is then sent to the encryption key manager 39 which generates an identical key based on the token. For example, the key can be updated every time the printer controller clears the print head decoder, after a particular number of print cycles, or after a particular number of state machine clock cycles. By increasing the number of encryption keys, the probability that the system will be compromised diminishes. Preferably, the selection of the encryption key is a function of the print head decoder. This is done because if one key is discovered, the print head decoder could still be made to print by instructing the decoder to use only the known (compromised) key. The print head decoder can be made to randomly select a key and force the printer controller to comply. Once the data is decrypted, it is vulnerable to monitoring or tampering. By sealing the decoder to the print head and using any suitable known tamper protection techniques, the data can be protected. Such techniques include incorporating the decoder on the same silicon substrate as the printing elements control, utilizing chip-on-board and encapsulation techniques to make the signals inaccessible, constructing a hybrid circuit in which the decoder and printing elements controls are in the same package, utilizing the inner routing layers of a multilayer circuit board to isolate the critical signals from unwanted monitoring, and fiber optic or opto-isolation means.

The provided description illustrates the preferred embodiment of the present invention and should not be viewed as limiting. The full scope of the invention is defined by the following claims.

Claims

1. A method for verifying a specific operable combination of postage metering controller to a remotely located digital printer over a communication link between the meter controller and the digital printer comprising the steps of:

   providing said meter with means for encrypting/decrypting data utilizing a encryption key:
   providing said digital printer with means for encrypting/decrypting postage data utilizing said encryption key;
   generating a random number and encrypting said random number at said digital printer:
   transmitting said encrypted random number to said meter;
   decrypting of said random number and re-encrypting said random number in such a way to have a known relationship to said original random number;
   transmitting said re-encrypted random number and known relationship to said digital printer;
   decrypting said re-encrypted random number and known relationship and verifying said relationship: and
   enabling said digital printer upon verification.

2. A method for verifying a specific operable combination of postage metering controller to a remotely located digital printer over a communication link between the meter controller and the digital printer as claim in claim 1, further comprising the steps of:

   providing said postage metering vault with a encryption key manager for generating an encryption key pursuant to a token:
   providing said digital printer with means of generating said token:
   communicating said token to said postage meter vault: and
   generating a encryption key by said encryption key manager in said postage meter vault pursuant to said token such that said encryption key of both of said encryption key managers are identical.

3. A postage metering system having a postage meter remote from a digital printer used to print said postage indicia, comprising:

   said postage meter having a micro controller and encryption-decryption means for encrypt-

ing and decrypting data pursuant to a encryption key in response to command signals from said micro controller:
said digital printer having decrypting-encryption means for encrypting and decrypting data pursuant to a encryption key in response to command signals from said micro controller:
communication means for communicating data between said postage meter and said digital printer;
said digital printer having means for generating a random number and causing said random number to be encrypted and causing said communication means to communicate said random number to said encryption-decryption means of said meter,
said micro controller having means for causing said encryption-decryption means to decrypt said random number and encode said random number in a desired relationship to said random number and causing said encoded random number and said relationship and causing said encryption-decryption means to encrypt said encoded random number and numeric relationship and cause said communication means to communicate encoded random number and said relationship to said decryption-encryption means: and
said printer decryption-encryption means having verification means for verifying said decrypted encoded random number and said relationship and enable said digital printer if verification is successful.

4. A postage metering system having a postage meter remote from a digital printer used to print said postage indicia as claimed in claim 3, further comprising:

said postage meter having a encryption key manager means for generating an encryption key in response to a token:
said digital printer having a encryption key manager means for generating a new encryption key, when desired, as a function of said decrypted data, and generating said token as a function of said decrypted data: and
communication means for electronically communicating said token to said postage meter encryption key manager.

5. A postage metering system having a postage meter remote from a digital printer used to print said postage indicia as claimed in claim 3, further comprising:

said postage meter having a encryption key manager means for generating an encryption key in response to a token;
said digital printer having a encryption key manager means for generating a new encryption key, when desired, as a function of a randomly generated token: and
communication means for electronically communicating said token to said postage meter encryption key manager.

6. A method for verifying a specific operable combination of postage metering controller to a remotely located digital printer over a communication link between the meter controller and the digital printer, comprising the steps of:

generating a random number and encrypting said random number at said digital printer:
transmitting said encrypted random number to said meter;
decrypting said random number and re-encrypting said random number in such a way to have a known relationship to said original random number;
transmitting said re-encrypted random number and known relationship to said digital printer;
decrypting said re-encrypted random number and known relationship and verifying said relationship: and
enabling said digital printer upon verification.

7. A method according to claim 6, further comprising the steps of:

generating in said digital printer a token representing a specific decryption key:
communicating said token to said postage meter: and
generating an encryption key in said postage meter pursuant to said token such that said encryption keys of said digital printer and said postage meter are identical.

8. A postage metering system comprising a digital printer (21) used to print postage indicia, a postage meter (11) remote from said digital printer (21), and communication means (C11) for communicating data between said postage meter (11) and said digital printer (21):

said postage meter having a micro controller (13) and encryption-decryption means (18) for encrypting and decrypting data pursuant to an encryption key in response to command signals from said micro controller (13):
said digital printer (21) having decryption-encryption means (25) for encrypting and decrypting data pursuant to an encryption key in response to command signals from said micro

controller (13);
said digital printer also having means (66) for generating a random number and for causing said decryption-encryption means (25) of said digital printer (21) to encrypt said random number and cause said communication means (C11) to communicate said random number to said encryption-decryption means (18) of said meter (11),
said micro controller (13) having means for causing said encryption-decryption means (18) of said meter (11) to decrypt said random number and encode said random number in a desired relationship to said random number and causing said communication means (C11) to communicate said encoded random number and said relationship to said decryption-encryption means (25) of said printer (21); and
said printer decryption-encryption means (25) of said printer (21) having verification means (66) for verifying said decrypted encoded random number and said relationship and for enabling said digital printer (21) if verification is successful.

9. A postage metering system according to claim 8, wherein

said digital printer (21) has an encryption key manager means (61) for generating a new encryption key, when desired, as a function of printer operation and for generating a token representing said new encryption key; and
said postage meter (10) has an encryption key manager means (3a) for generating an identical encryption key in response to receipt of said token communicated electronically over said communication means (C11), from said printer encryption key manager (61).

10. A postage metering system according to claim 8, wherein:

said digital printer (21) has an encryption key manager means (61) for generating a new encryption key, when desired, as a randomly selected key and for generating a token representing said new encryption key; and
said postage meter (10) has an encryption key manager means (39) for generating an identical encryption key in response to receipt of said token communicated electronically over said communication means (C11), from said printer encryption key manager (61).

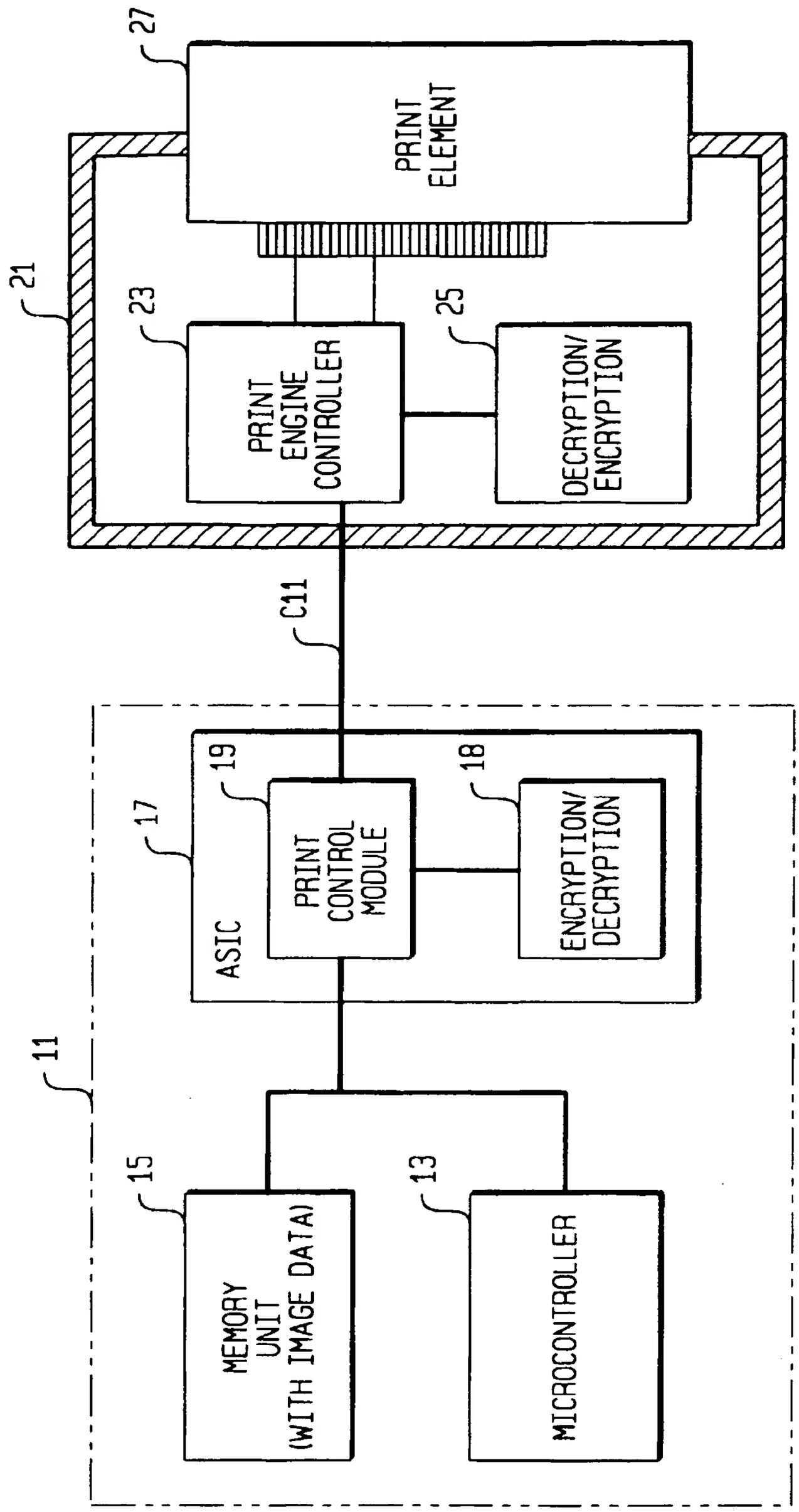
27
PRINT ELEMENT
21
23
PRINT ENGINE CONTROLLER
25
DECRYPTION/ ENCRYPTION
C11
11
17
ASIC
19
PRINT CONTROL MODULE
18
ENCRYPTION/ DECRYPTION
15
MEMORY UNIT (WITH IMAGE DATA)
13
MICROCONTROLLER

FIG. 1

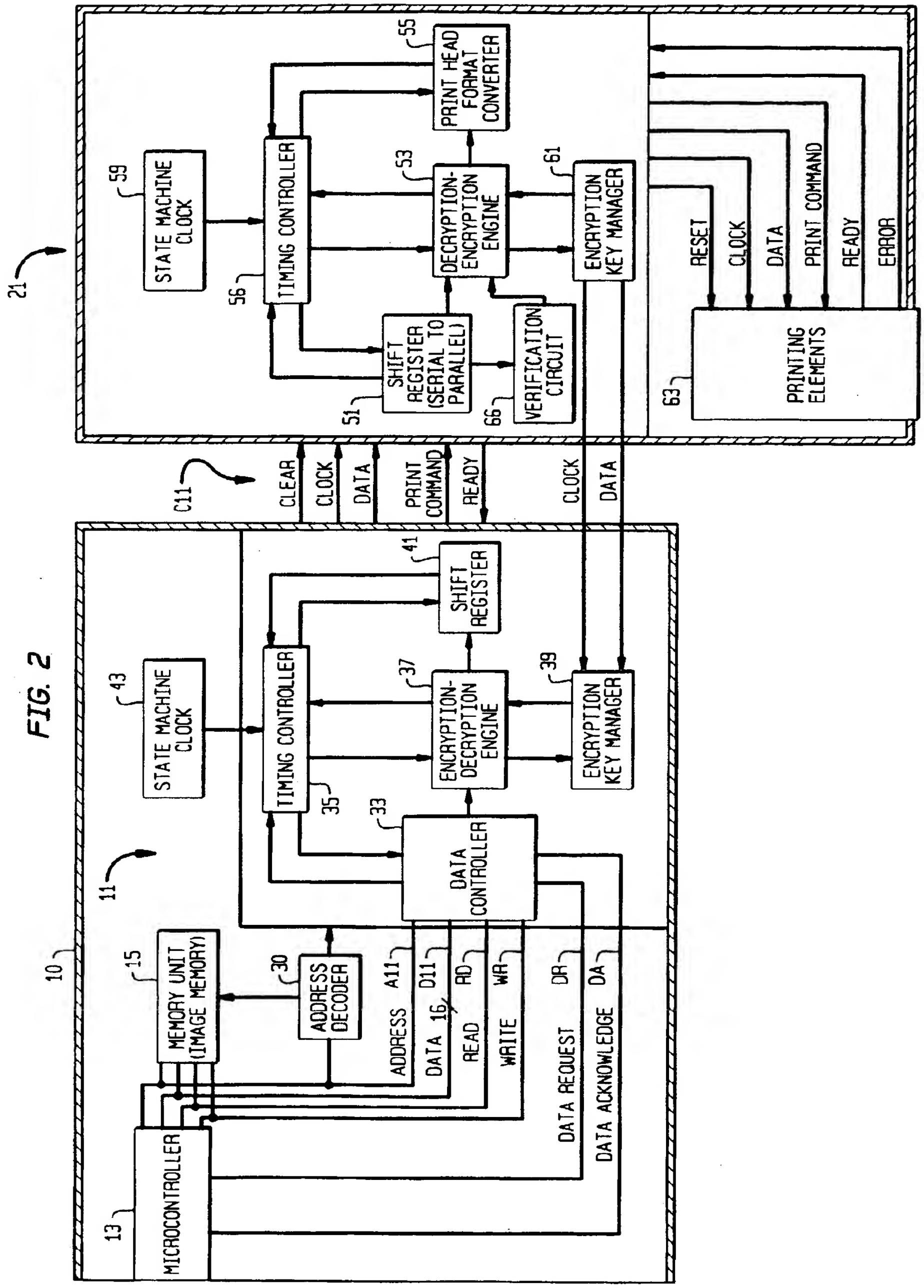
21
STATE MACHINE CLOCK
59
TIMING CONTROLLER
56
PRINT HEAD FORMAT CONVERTER
55
DECRYPTION-ENCRYPTION ENGINE
53
ENCRYPTION KEY MANAGER
61
SHIFT REGISTER (SERIAL TO PARALLEL)
51
VERIFICATION CIRCUIT
66
RESET
CLOCK
DATA
PRINT COMMAND
READY
ERROR
PRINTING ELEMENTS
63
C11
CLEAR
CLOCK
DATA
PRINT COMMAND
READY
CLOCK
DATA
11
STATE MACHINE CLOCK
43
TIMING CONTROLLER
35
SHIFT REGISTER
41
ENCRYPTION-DECRYPTION ENGINE
37
ENCRYPTION KEY MANAGER
39
DATA CONTROLLER
33
10
MEMORY UNIT (IMAGE MEMORY)
15
ADDRESS DECODER
30
MICROCONTROLLER
13
ADDRESS A11
DATA 16
D11
READ
RD
WRITE
WR
DATA REQUEST
DR
DATA ACKNOWLEDGE
DA

FIG. 2

(19) Europäisches Patentamt
Europ an Patent Office
Office européen des brevets

(11) EP 0 718 803 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
27.10.1999 Bulletin 1999/43

(43) Date of publication A2:
26.06.1996 Bulletin 1996/26

(21) Application number: **95120424.7**

(22) Date of filing: **22.12.1995**

(51) Int Cl.[6]: **G07B 17/04**

(84) Designated Contracting States:
DE FR GB

(30) Priority: **22.12.1994 US 361409**

(71) Applicant: **PITNEY BOWES INC.**
Stamford Connecticut 06926-0700 (US)

(72) Inventors:
- **Lee, Young W.**
  Orange, Connecticut 06477 (US)
- **Moh, Sungwon**
  Wilton, Connecticut 06897 (US)
- **Muller, Arno**
  Westport, Connecticut 06880 (US)

(74) Representative: **Avery, Stephen John et al**
Hoffmann Eitle,
Patent- und Rechtsanwälte,
Arabellastrasse 4
81925 München (DE)

(54) Identifying a specific combination of metering accounting vault and digital printer

(57) For preventing monitoring of postage indicia data which is sent from a postage metering vault to a remotely located digital printer (21) over a communication link (C11) between the meter vault and the digital printer (21), the meter (11) is provided with an encryption engine (37) for encrypting postage indicia data utilizing an encryption key. The digital printer (21) includes a decryption engine (53) for decrypting postage data received from said meter (11) utilizing the same encryption key and then prints a postage indicia pursuant to the decrypted postage indicia data. The postage meter (11) also includes a key manager (39) for generating new encryption key pursuant to a token which is either randomly generated or generated pursuant to an algorithm by a similar encryption key manager (61) located in the digital printer (21), which token is also used to generate the decryption key for the decryption engine (53). As a result, the encryption keys are the same. Upon power-up of the system or at such other preselected times, the print controller module of the digital printer (21) sends out an encrypted message to the meter (11). The message consist of a random number. The encryption/decryption engine (37) of the vault decrypts the message. The vault then returns an encrypted new message to the print controller (23) which includes an encoded representation of the relationship of the two messages. Upon receiving the new message from the vault, the print controller (23) decrypts the new message and verifies the relationship. The print controller (23) is then enabled to print a postage indicia.

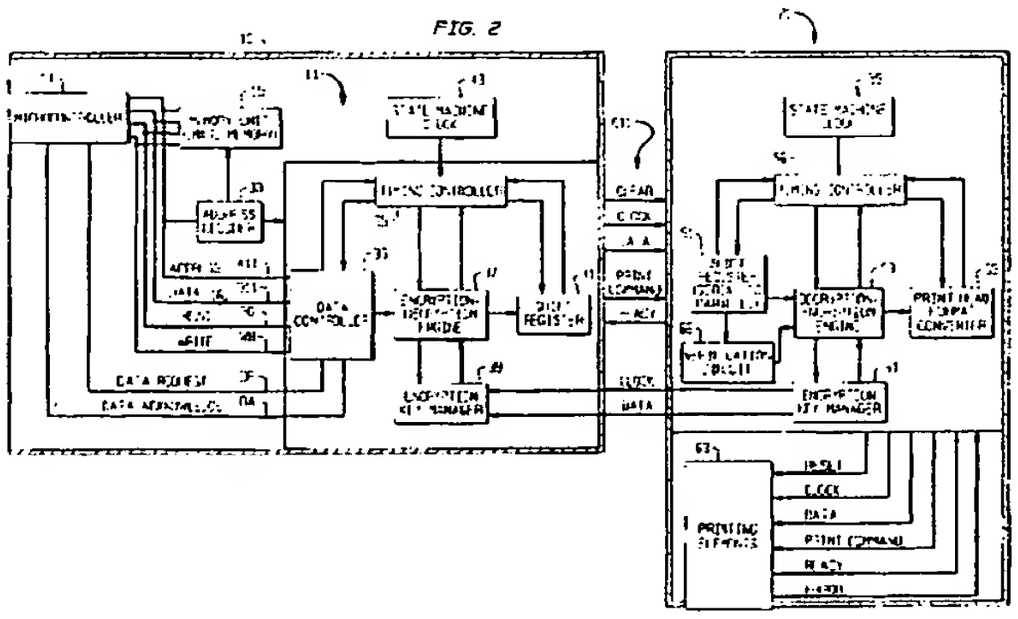

FIG. 2

EP 0 718 803 A3

Printed by Jouve, 75001 PARIS (FR)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 95 12 0424

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
Y A	EP 0 522 809 A (NEOPOST LTD) 13 January 1993 (1993-01-13) * column 3, line 17 - column 4, line 56 * * abstract; claims 1-8; figures 1,2 *	1,3,6,8 2,4,5,7,9,10	G07B17/04
Y A	US 4 876 716 A (OKAMOTO EIJI) 24 October 1989 (1989-10-24) * column 1, line 48 - column 2, line 44 * * claims 1,5,9,11; figure 1 *	1,3,6,8 2,4,5,7,9,10	
A	US 4 935 961 A (GARGIULO JOSEPH L ET AL) 19 June 1990 (1990-06-19) * column 1, line 39 - column 3, line 38 * * abstract; claims 1-9; figures 3,5 *	1-10	
A	EP 0 018 081 A (PITNEY BOWES) 29 October 1980 (1980-10-29) * page 2, line 17 - page 4, line 12 *	1-10	

TECHNICAL FIELDS SEARCHED (Int.Cl.6)

G07B
H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	2 September 1999	Reule, D

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 95 12 0424

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

02-09-1999

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0522809 A	13-01-1993	DE 69223866 D	12-02-1998
		DE 69223866 T	28-05-1998
		US 5293465 A	08-03-1994
US 4876716 A	24-10-1989	JP 1871933 C	26-09-1994
		JP 4056501 B	08-09-1992
		JP 63054037 A	08-03-1988
		JP 1871934 C	26-09-1994
		JP 4056502 B	08-09-1992
		JP 63054038 A	08-03-1988
		CA 1279709 A	29-01-1991
		DE 3782780 A	07-01-1993
		EP 0257585 A	02-03-1988
US 4935961 A	19-06-1990	NONE	
EP 0018081 A	29-10-1980	US 4253158 A	24-02-1981
		CA 1129554 A	10-08-1982
		JP 1483778 C	27-02-1989
		JP 55131867 A	14-10-1980
		JP 63031820 B	27-06-1988

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82